



Langslide

Data and Record Retention and Deletion Policy

Version 1.0

PURPOSE

To ensure storage and retention of information, data, and records as per contractual and legal requirements and protection from loss, falsification, destruction, unauthorized access, and unauthorized release.

SCOPE

This policy applies to Rudramsa Systems Pvt. Ltd. (hereinafter referred to as Organization), its employees, contractors, and operations.

DEFINITION

Following is an explanation of various terms used within this document –

- **ISMS:** Information Security Management System
- **Information Security:** Confidentiality, Integrity, Availability of information.
- **CEO:** Chief Executive Officer
- **LT:** Leadership Team
- **ISG:** Information Security Group
- **Information:** Meaningful Data
- **PII:** Personally Identifiable Information
- **Electronic Data:** Emails, Databases, Files, Scanned Images, and Data in storage devices such as Hard Disks, USB Drives, Tapes, etc.
- **Non-Electronic Data:** Hard Copy Documents, Printed Documents.
- **Record:** Paper files, electronic documents, correspondence (including letters, faxes, and emails), and data used in business applications and databases. Retention: Records retention is the term applied to the safeguarding of important records that document decisions, policies, financial activities, and internal controls. A retention period is an aspect of records that identifies the duration for which the information should be maintained or “retained,” irrespective of format (paper, electronic, or other).
- **Archival:** Archiving means separating records that are no longer actively utilized from active records. This usually means moving hard-copy records to an offsite storage facility. For digital records, archiving may involve updating the status and moving the record to a separate data storage.

RESPONSIBILITIES

- The primary responsibility for implementing this policy is to have all departments and teams handle data and records.
- The ISG shall implement this Policy under the guidance of the Leadership Team and in coordination with Department Heads.

POLICY

Identification and Classification of Data and Records

- All departments shall identify the data and records that they create or handle.

- All data and records belonging to Customers, External Persons, Entities, or Organizations shall also be identified under External Origin Data or Records.
- As shown below, organizational classification shall be applied to all data types and records. For more details, refer to the Information Classification Policy.
 - Confidential
 - Internal Use
 - Public
 - External Origin
- All types of data and records existing within the organization shall be identified and documented within the prescribed format, along with Custodian information and classification applied to the same. (Ref: Annexure A - Retention Schedule)

Retention Period of Data and Records

- The retention period for each type of data and record shall be defined and applied by the concerned Department that creates or handles the data or record.
- While deciding the retention period, the following sequence shall be followed –
- Check Statutory or Regulatory or Legislative requirement of retention for each type of Data or Record,
- Check if any Contractual requirement exists for the retention of each type of data or record,
- Check Organizational policy about retention of data or records,
- Select the highest applicable retention period and apply it to the data or record.
- In the case of externally provided data or records provided by an external person or entity, the retention period as specified by the external person or entity shall be referred to in addition to the above-listed sequence.
- The retention period defined and applied for each type of data and record shall also be applied to the backups / archival of concerned data or records.
- Records shall be appropriately archived during the retention period.
- Once applied to any data or record, the retention period shall not be changed without prior approval from the Leadership Team.
- The retention period for all types of data and records within the organization shall be defined and documented in the prescribed format. (Ref: Annexure A - Retention Schedule)

Protection of Data and Records

- Access to each type of Data or Record shall be provided based on its classification.
- The access provision and revocation to all types of data and records shall be governed by corresponding policies.
- Risks for records shall be assessed, and mitigation controls shall be implemented to protect the data and records.
- Electronic data and records shall be protected from unauthorized access, theft, disclosure, corruption, changes, destruction, etc. Adequate provisions shall be made regarding backup and redundancy of data and records in case of disaster.

Disposal / Deletion / Destruction of Data and Records

- Data and records shall be destroyed/deleted or disposed of securely when no longer required or at the end of the retention period to avoid unauthorized access.
- All electronic data and records shall be disposed of / destroyed using secure controls such as –
- Delete + Purge of Electronic Data and Records.
- The destruction, deletion, or disposal of data or records shall also apply to backup or archived copies at the end of the retention period.
- The concerned department shall retain records of the destruction, deletion, or disposal of Personal Data / PII / Confidential Information for future audits and reference.

ANNEXURE A - RETENTION SCHEDULE

Type of Data	Retention Period
Application and related database	
Client Personal data (Client Master setup in Products)	<ul style="list-style-type: none"> • Retain as long as the client contract continues or
	<ul style="list-style-type: none"> • Three months from the date of termination of the client contract or as specified in the client contract
Client's end-user data or employee data within the Application hosted on the cloud	<ul style="list-style-type: none"> • Retain as long as the client contract continues or • Three months from the date of termination of the client contract or as specified in the client contract
Client's data - Files and media within the cloud	<ul style="list-style-type: none"> • Retain as long as the client contract continues or • Three months from the date of termination of the client contract or as specified in the client contract
Backup of Database	<ul style="list-style-type: none"> • Retain as long as the client contract continues or • Three months from the date of termination of the client contract or as specified in the client contract
Trial Customer Data	<ul style="list-style-type: none"> • Delete within one month after the end of the trial
IT Infrastructure	
User Desktops/laptops	<ul style="list-style-type: none"> • Data on user desktops and laptops is deleted only when the user exits the company.

Type of Data	Retention Period
Employee-owned devices	<ul style="list-style-type: none"> Employees are encouraged not to store anything on employee-owned devices. These are out of the scope of the retention policy.
Data stored on cloud services	
Personal Drives	<ul style="list-style-type: none"> Personal drives are not permitted
Corporate Drives/archives such as Dropbox, One Drive	<ul style="list-style-type: none"> Corporate drives are not in use. If used, the retention period is determined by the data type.
Client Data - Hard Copies	
Client Data - Hard Copies	<ul style="list-style-type: none"> Within 30 days or as per contractual/ regulatory requirements
Offline payroll Processing Services	
Excel input files received from clients and input within the application	<ul style="list-style-type: none"> As per regulatory requirements
Output files, if any, sent to clients	<ul style="list-style-type: none"> Retain for 7 years or one year from the termination date of the client contract, whichever is earlier.
Marketing	
CRM	<ul style="list-style-type: none"> All active Contacts are to be retained until they Opt-out.
	<ul style="list-style-type: none"> On opt out, retain bare minimum data and delete other data.
	<ul style="list-style-type: none"> Dormant contacts – inactive for the last 2 years are deleted.
For Marketing	<ul style="list-style-type: none"> Mailing List retention is the same as CRM data

Type of Data	Retention Period
	<ul style="list-style-type: none"> • Opt-out list retained forever
Client Communication	<ul style="list-style-type: none"> • Not retained – API call
Finance	
Invoices on <Tool name>	<ul style="list-style-type: none"> • As per statutory limits applicable in the region
Client Master data on <Tool name>	<ul style="list-style-type: none"> • Retain as long as the client contracts in place.
Website	
Cookie Data	<ul style="list-style-type: none"> • Retain for 180 to 365 days

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya